数据包分析工具及其在网络管理中的应用

摘　要：伴随着计算机网络的高速发展，我们能够迅速获取最新的信息和知识，人们的工作和生活发生了巨大的变化，越来越依赖网络，对网络的安全性也越来越重视。数据包是网络通信传输中的重要数据单位，因此，数据包分析技术的运用对保障网络的高效、稳定、可靠运行有积极的意义。数据包分析工具的作用就是帮助网络管理员监控网络性能、分析网络安全状况、定位各类网络相关问题。本文简要介绍了数据包分析技术原理等相关知识，展示了数据包分析工具在网络管理工作中的部分实践经验。

关键词：数据包分析；原理；网络管理
中图分类号：TP393　　文献标识码：A
文章编号：1671-0134（2019）02-125-03　　DOI：10.19483/j.cnki.11-4653/n.2019.02.032

文 / 张智伟

chinaXiv:202310.01732v1

在庞大的互联世界里，承载着各种信息的数据包通过网络时刻不停地交换传递，往来于不同的目的地，数据包被不同的人赋予了不同的用处，有的传送数据，有的暗藏危险，不明身份的数据包到处游荡给网络安全带来了隐患。为了能够清晰地了解网络中数据包携带的信息，我们需要运用数据包分析技术对它们进行解读，以分析网络中的细微变化，提前做好安全防范，及时定位、清理网络中的风险。

为了能够掌握网络数据包的真实状况，网络管理工作通常会借助数据包分析工具抓取信息后生成的大量数据统计信息，对网络上的通信设备及传输进行有效的还原，及时清理影响安全运行的故障或隐患。

目前，市面上有很多流行的数据包分析工具，如OminiPeek、Sniffer Pro、Wireshark、Tcpdump/windump、国产科来等，功能上略有差异，这些软件有商业的、有免费的，可按个人喜好选择使用。

1. 数据包分析工具简介

1.1 原理

数据包分析工具的本质是数据包嗅探，是观察正在运行的协议实体间交换报文的基本工具，通常用来进行协议分析和网络监控，以便进行故障诊断、性能分析和安全分析等，黑客则用它进行安全敏感信息的监听和截取。

数据包分析工具主要由分组捕获器（packet capture）和分组分析器（packet analyzer）两部分组成。

分组捕获器需要把网卡设置为“混杂模式（promiscuous mode）”，当数据包从嗅探器所连接的网卡上进入系统时，嗅探程序可以收到整个以太网内的网络数据信息，包括所有的广播、组播和单播数据包，甚至错误数据包，从而实现数据包捕获。

分组分析器的作用是分析协议报文并把报文中所有的字段内容直观地显示出来。其主要构成通常包括包过滤器、数据包缓冲区和解码部分，包过滤器用于设定协议分析器想要捕获的数据包类型，通常都可以按照协议类型、通信的 IP 地址、网络接口层地址和应用程序来设定过滤条件；解码部分主要是将缓冲区中已经捕获的数据包解析为用户可读的协议数据单元格式，以便用户分析。

绝大多数数据包分析工具都提供了一定的数据包统计功能，可以对各种类型的数据包进行整理统计，包括各种类型的错误数据包。

1.2 主要用途

数据包分析工具在网络管理中通常用于诊断网络活动出现的故障，还可以用于搜集网络性能的趋势，从而为预防出现影响网络正常工作或性能的极端情况提供参考，多数数据分析包工具都有能力跟踪网络流量的短期和长期趋势，包括网络利用率、每秒钟数据包速率、数据包长度分布及使用的协议等，网络管理员能够利用这些信息跟踪网络发生的细微变化，为网络管理提供极大的帮助。

1.3 部署方式

常见的数据包分析工具部署方式有 3 种：

（1）直接在被监控的主机上安装，用来捕获通过网卡进出的所有数据包。

（2）端口镜像。将交换机上的多个端口镜像到一个端口用于监控。

采用端口镜像方式时，需要注意镜像端口的流量负载，把太多的端口镜像到一个端口，在网络流量达到一定级别后，可能会远远超出镜像端口的物理承受能力而出现数据包丢失情况，而且交换机在长时间维持最大负

荷时，可能会将镜像端口判断为遭到某类型的拒绝服务或广播风暴攻击，丢弃多余的数据包，甚至暂停内部交换电路。在高吞吐量级别的环境下，端口镜像可能会产生不稳定的结果。

（3）使用网络分路器（TAP）。网络分路器是一个可以实时获取网络流量的硬件设备，使用时串接在网络链路中，在不影响网络正常流量的情况下，将被监测链路中的网络数据复制到它的另外一个或多个端口上供不同的分析工具进行分析。

只有正确捕获数据包，才能如实还原网络的状况，在部署数据包分析交换工具时还是要先了解抓包网络的具体情况，仔细考虑工具的部署位置。有些特殊情况应当注意：在交换式网络中，抓取整个 VLAN 数据包，须直连核心交换机，避免因特殊 VLAN 划分导致部分主机数据包漏抓；防火墙流量监控有所不同。监控防火墙内口，可以观察到内网用户发起的所有访问 Internet 的流量，其源 IP 地址均为内部 IP 地址，监控防火墙外口，则观察到的是所有经过防火墙放行的访问 Internet 的流量，其源 IP 地址均为外部（公网）地址。

2. 网络管理应用

通过数据包分析工具可以查看网络中的通信过程及应用占用带宽情况，识别网络运行的高峰时间，分析可能的攻击或恶意行为，寻找不安全以及滥用网络资源的应用，是了解网络状况的最佳工具。日常网络管理应用大多基于以下几个方面：

2.1 评估网络性能

数据包分析工具内置了多种数据统计信息功能，如 IO、协议分层、会话等数据汇总图表，通过这些信息展示出当前网络数据包所呈现的带宽性能、用户带宽占用、数据包长度、端点会话情况等综合情况，为网络管理员分析、评估是否要对网络进行相应的调整提供了详实的数据依据。

在传输期间发生错误、丢包、重传现象，是网络管理员在工作中需要关注的常见问题。其中，遇到最多的是 TCP 重传，这种情况下，可记下报错 IP 地址，然后直接在浏览器访问，能访问的可根据网页信息判断与网络内的终端是否有应用关联；无法访问的可以到域名查询网站（如 whois.com）了解该 IP 的注册信息，再做进一步处理。

实际工作中，也经常遇到与应用层软件有关的情况，例如，一种是终端用户使用了一些部分功能可在国内使用的境外软件，运行中后台自动访问不能在国内访问的境外官网，导致无法连接出现错误数据包。最典型的是谷歌，其 Chrome 浏览器市场占有率较大，内置的某些模块经常会后台访问官网，运行 netstat 可以看到，前述方法查证的谷歌所属 IP 的 TCP 连接状态显示为 SYN_SENT，没有收到应答。一般情况下，TCP 三次 SYN 同步请求而没有任何回复，可能是服务器端的问题，也有可能是防火墙拦截了特定端口上的请求，大量访问谷歌地址产生的错误 TCP 数据包就应该属于这种情况。

又如，越来越多的杀毒、文字处理等各种应用软件厂家怀着不同的目的，以为用户提供各种服务为由，常驻电脑启动项或服务项，经常自动在后台连接其官网检查更新或同步数据。通过直接访问或 whois 查询的方式，确认其公网 IP 地址后，抓取客户端和服务器会话的数据包查看，双方第一次握手的 TCP SYN 同步请求都很快连接，但服务器回应客户端较慢，导致传输时发生 TCP 重传，推测为由于办公类软件互联网用户数量庞大，服务器连接压力较大。为了进一步确认发生 TCP 重传的 IP 地址所关联的应用层程序，运行 netstat –ano 查询该 IP 地址使用的 PID，使用进程查看工具强行关闭 PID 后，再次抓包，该地址不再出现在 TCP 重传统计里，由此可验证，应用层软件与 IP 地址的关系判断正确与否。

网络的性能受多种因素影响，不可能始终保持最佳状态，有赖于 TCP 的错误恢复特性，量级较小的延时、较少的 TCP 重复确认和重传等数据包错误，不需要做什么特别处理。

2.2 快速定位故障

曾经有用户反映在单位内网可以访问互联网，在抓包中发现网络中有单位内网地址主机的数据包，虽然内网规模较小，没有做 VLAN 划分等区分措施，但是各个内网主机分布在办公楼的各楼层，只能在机房汇聚交换机上一层一层拔除各楼层上连到交换机端口的网线，逐步缩小范围，确认混插位置。事后得知，该部门某人因无法上网，查看线路时看到部门的 8 口小交换机旁有网线，以为是从交换机上脱落，随手将网线插入了内网用的交换机，而这根网线实际上是从外网交换机上来的。

2.3 排查网络威胁

作为网络管理员，要时刻留意网络中可能出现的安全威胁，不定期观察网络数据包情况以及数据包分析工具内置的协议、会话、端点等统计信息，可清楚地观察到数据包在网络中的异动，我们可根据需要具体分析。使用统计信息时应当注意的是以下两点：

2.3.1 关注网络流量大的 IP 地址

有些异常的网络流量可以通过每个 IP 地址的收发包数量是否正常来判断，即收发之间是否存在较大差异，如发包数量远大于收包数量。光发包不收包是种类似于广播的应用，如果只收不发或者只发不收，那很可能就

chinaXiv:202310.01732v1

chinaXiv:202310.01732v1

意味着这个 IP 地址的当前流量有异常（例如受到 SYN 攻击），需要可以进一步通对捕获的数据包的内容进行分析。

2.3.2 分析大流量 IP 地址的数据包

查看大流量 IP 地址的协议使用和收发包情况，注意发包时间间隔，非常短的毫秒级间隔，异常流量包括 ARP、IP 或 TCP 扫描等，而 TCP 扫描行为未必只有病毒才能引发，软件 bug 也可以触发，应当注意区分。

由于感染病毒的主机会在网络中不断的发送数据包，使网络的效率非常低，大大影响网络的性能，利用数据包分析工具能非常直观、快速地发现这些主机，帮助网络管理人员迅速锁定问题 IP 地址。

查看 IP 对话统计信息，按照发出数据包由少到多排序，当看到一个 IP 地址向各个其他 IP 地址发送报文，就要注意继续确认是否有主机感染了病毒。

在 TCP/UDP 会话统计中可以查看发包，一般一个主机合理的 TCP 连接数是 10 到 30 个左右，上百个可能是不正常的，但也有可能是该主机正在进行 P2P 下载，需要核实。

结语

数据包分析工具能使我们更加深入地理解网络概念，清晰地了解网络层、传输层和应用层协议，快速地诊断网络故障，迅速解决网络的实际问题，在网络管理和安全监控中起到了很大作用。除此之外，数据包分析工具还可以应用于网络应用的开发与调试，帮助开发人员分析网络产品的数据包通信情况，以便于更好地优化产品。随着万物互联时代的到来，网络数据包分析工具的应用范围必将会越来越广阔。媒

参考文献

[1] 陈年 .TCP/IP 协议分析教程与实验 [M]. 清华大学出版社，2016：10-11

[2]（美）Chris Sanders 著，诸葛建伟，陆宇翔，曾浩辰，译 .Wireshark 数据包分析实战（第 3 版）. 人民邮电出版社，2018.

[3]Wireshark User’s Guide[EB/OL].https：//www.wireshark.org/docs/wsug_html_chunked/.

（作者单位：新华社北京分社）

（上接第 121 页）

地天气动态图；教育节目类制作同样离不开虚拟技术的融入。为了能够帮助学生更为全面和生动理解节目讲解的相关内容，通常将虚拟技术应用于演播室讲解过程中，运用三维动画形式等技术呈现所讲解内容，实现虚拟技术与教育场景的融合。不同的课程内容呈现方式有所不同，如对于人文历史类的知识而言，常运用虚拟技术呈现历史故事、历史中的人物以及经典典故等；对于科学理工类的知识，运用虚拟技术模拟实验操作过程和结果，节省了开展实验的时间和大量资源等。虚拟技术的应用丰富了教学效果，也激发了学生对节目内容的兴趣度。

4. 虚拟技术在电视节目制作中应用的启示

4.1 适度应用虚拟技术

随着虚拟技术在我国各个领域应用范围的不断拓展，滥用和错用技术等情况经常发生。如滥用错用虚拟技术使电视节目原有的效果受到负面影响。如台湾壹电视滥用虚拟技术播放杀人、自身等现场内容，还原了现场细节和过程，对未成年人的身心健康发展形成了不良影响。因此，虚拟技术在应用的过程中应追求真实性和合法性等原则，向社会公众传递社会正能量。

4.2 挖掘虚拟技术的潜能

随着虚拟技术在电视节目制作过程中的广泛使用，虚拟技术的内在潜能得到逐步挖掘。因此，为了进一步丰富电视节目的制作过程，还应当培养综合型人才，运用所学的专业知识和技术挖掘诸多未被挖掘的虚拟技术，积极地将技术应用于电视节目的制作之中。

总而言之，虚拟技术在电视节目制作过程中的应用充分展示了电视制作技术的升级和发展，在应用过程中应遵循合法性和真实性原则，使技术与电视节目实现融合，为广大受众提供盛大的视觉盛宴。媒

参考文献

[1] 范清淳 . 多媒体技术在电视节目制作中的应用 [J]. 传播力研究，2018（8）：93-95.

[2] 敖建华 . 基于虚拟现实技术的电视节目制作 [J]. 西部广播电视，2018（6）：104-106.

[3] 闫金霞 . 数字化编辑技术在电视节目制作中的作用 [J]. 科技传播，2018（6）：30-32.

[4] 牛莊 . 计算机技术在电视节目制作中的应用 [J]. 西部广播电视，2018（1）：55-58.

[5] 王莹 .VR 技术在电视节目制作中的探索与应用 [J]. 长春师范大学学报，2018（6）：33-34.

（作者单位：辽宁广播电视台）